LIETUVOS RESPUBLIKOS VALSTYBĖS KONTROLĖ

VALSTYBINIO AUDITO ATASKAITA
FINANSŲ MINISTERIJOS INFORMACINIŲ SISTEMŲ BENDROJI IR KŪRIMO KONTROLĖ

2012 m. liepos 16 d. Nr. VA-P-90-1-9
Vilnius

Auditas atliktas, vykdant 2011-07-11 pavedimą Nr. P-90-1

Auditą atliko valstybinių auditorių grupė:
Aurelija Martinkutė (grupės vadovė)
Irina Kiškina
Jurgita Musteikienė
Kęstutis Kumetaitis

Auditas pradėtas 2011-07-11
Auditas baigtas 2012-07-16

Su valstybinio audito ataskaita galima susipažinti
Valstybės kontrolės interneto puslapyje
adresu www.vkontrole.lt

SANTRAUKA

Valstybės kontrolė atliko Finansų ministerijos informacinių sistemų bendrosios ir kūrimo kontrolės auditą. Auditas apėmė 2008–2011 m. laikotarpį, kai kuriais atvejais palyginimui buvo naudojami ir ankstesnių metų duomenys.

Finansų ministerija, automatizuodama savo veiklos funkcijas, nuo 1995 m. naudoja įvairaus sudėtingumo informacines sistemas. Audituojamu laikotarpiu ministerijoje veikė dešimt informacinių sistemų, kurių naudotojai – daugiau nei 4000 viešojo sektoriaus institucijų ir įstaigų. Bendrosios kontrolės auditui atlikti pasirinktos keturios visai valstybei svarbią informaciją apdorojančios informacinės sistemos, skirtos ministerijos ir valstybės piniginiams ištekliams valdyti.

Planuojant, kuriant ir valdant reikšmingas valstybei informacines sistemas (IS), reikalingos informacinių technologijų (IT) strateginio planavimo ir valdymo žinios, sugebėjimas susieti veiklos poreikius su IT teikiamomis galimybėmis, optimaliai naudoti IT, siekiant veiklos efektyvumo. Daugelis IT valdymo aspektų (išskyrus saugą, IS kūrimą, eksploatavimą, investicijų planavimą) buvo aprašyti tik gerųjų praktikų rekomendacijose, tačiau iki 2012 m. sausio 1 d. nebuvo privalomojo pobūdžio. Nuo šių metų pradžios įsigaliojus Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymui[1], institucijos, valdančios ypatingos svarbos valstybės informacinius išteklius, privalo rengti IT plėtros planus, atlikti informacinių technologijų auditus[2] ir vykdyti kitas gerųjų praktikų rekomendacijas, perkeltas į įstatymą ir poįstatyminius teisės aktus.

Finansų ministerija, siekdama geresnio IT poveikio, audituojamu laikotarpiu savo veikloje vadovavosi tarptautinių IT valdymo metodikų (COBIT[3] ir ITIL[4]) rekomendacijomis, tačiau tam tikrų šiose metodikose nurodytų procesų taikymas nebuvo rezultatyvus. Pagal šių metodikų rekomendacijas Finansų ministerija 2004 m. sudarė IT valdymo komitetą. Jo pagrindinės funkcijos – IT strategijos tvirtinimas ir įgyvendinimo priežiūra, tačiau audituojamu laikotarpiu buvo patvirtinta tik 2008–2010 m. IT strategija, o komitetas buvo susirinkęs tik du kartus. 2008–2010 m. strategijoje buvo numatyta strategijos įgyvendinimo rizikos, informacijos saugos ir kiti principai, tačiau strategija neapėmė visų tuo metu ministerijoje kuriamų informacinių sistemų.

Audito metu nustatyta, kad ministerijos elektroninės informacijos valdymas turi trūkumų: nėra detalaus elektroninės informacijos klasifikavimo aprašymo ir informacijos priskyrimo kriterijų, todėl suteikus prieigą prie elektroninių duomenų ministerijos darbuotojams, kuriems šie duomenys nereikalingi tiesioginėms pareigoms atlikti, gali būti atskleista, sunaikinta arba pakeista Finansų

[1] Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807.
[2] Ten pat, 9 ir 14 str.
[3] COBIT 4.1., 2011 m. Vilnius.
[4] ITIL (angl. *Information Technology Infrastructure Library*) – IT paslaugų valdymo metodika ir geroji praktika.

ministerijos kaupiama informacija. Nenumatytos reikiamos Valstybės iždo finansų valdymo ir apskaitos informacinės sistemos (FVIS) ir Finansų valdymo ir apskaitos informacinės sistemos (FVAIS) saugai ir tęstinumo užtikrinimui skirtos priemonės, nes, auditorių nuomone, šios sistemos turėtų būti priskirtos aukštesnėms kategorijoms.

Taip pat nustatyta, kad ministerijoje periodiškai nebuvo atliekami ministerijos informacinių sistemų rizikos ir IS saugos atitikties vertinimai, neatnaujinti saugos politiką ir jos įgyvendinimą reglamentuojantys dokumentai, neišbandytos IS kontrolės priemonės, užtikrinančios pasirengimą nuosekliai ir efektyviai atkurti IS veiklą, esant nenumatytoms situacijoms, nenustatyta dalis asmens duomenų saugumo priemonių, neužtikrintas nuoseklus incidentų valdymas ir Lietuvos Respublikos teisės aktų nuostatų įgyvendinimas (žr. 3 ir 4 priedus). Dėl audito metu nustatytų informacinių technologijų saugumo trūkumų kyla rizika Finansų ministerijos veikloms, užtikrinančioms ministerijos ir valstybės piniginių išteklių valdymą, taip pat kitų kompiuterizuotų funkcijų vykdymui.

Atsižvelgdami į audito metu nustatytus faktus auditoriai nustatė, kad Finansų ministerijos IS vidaus kontrolės branda pagal Gebos brandos modelį (angl. *Capability Maturity Model,* CMM) apibrėžiama kaip Pirminis / *Ad-Hoc* (1) procesas (žr. 3 pav. ir 5 priedą). Norint pasiekti aukštesnį brandos lygį ministerijoje IT valdymo komiteto veikla turėtų būti rezultatyvesnė, IT strategija turi tapti nuolatiniu veiklos gerinimo procesu, siejant ją su veiklos pokyčiais ir vertinant jos įgyvendinimą. Turi būti dokumentuotos IT veiklos procedūros (pvz., pokyčių ir incidentų valdymas ir kt.), o esama dokumentacija turi būti nuolat atnaujinama ir atitikti realią situaciją. Periodiškai turi būti vertinama rizika ir IS saugos atitiktis, užtikrinama vykdomų procesų stebėsena.

Finansų ministerija neužtikrino efektyvaus VSAKIS kūrimo, nes sistema kurta nepatvirtinus specifikacijos – nenustačius techninių reikalavimų kuriamai sistemai ir ekonominio pagrindimo, kaip reikalauja teisės aktai, o projekto įgyvendinimas vėlavo 13 proc. viso numatyto projekto vykdymo laiko. Nors ministerija skyrė daug dėmesio projekto kokybei užtikrinti, nustatyti nedetalūs ir nepamatuojami projekto tikslų pasiekimo kriterijai buvo nepakankami įvertinti projekto rezultatų sukuriamą vertę.

Išvados

1. IT planavimas yra nepakankamas ir neatspindi veiklos poreikių, IT valdymo komiteto veikla nerezultatyvi, IT strategijos tvirtinamos fragmentiškai, neperžiūrimos ir nevertinamas jų įgyvendinimas, todėl Finansų ministerijos IT valdymo brandos lygis yra Pirminis (1.1 poskyris).

2. Ministerijoje nustatyta IT saugos trūkumų, nes:

2.1. įgyvendintos ne visos teisės aktuose reikalaujamos organizacinės ir techninės asmens duomenų saugumo priemonės, skirtos apsaugoti asmens duomenims, todėl neužtikrinamas

numatytas saugos lygis ir kyla grėsmė, kad asmens duomenys gali būti atsitiktinai sunaikinti, pakeisti arba atskleisti (1.4 poskyris);

2.2. saugos įgaliotinis kasmet neorganizavo visų IS rizikos įvertinimo, todėl IS rizikos valdymo sistema turi trūkumų ir neatitinka teisės aktų reikalavimų – numatytu periodiškumu nevertinti veiksniai, galintys turėti įtakos informacijos saugai, dalis rizikos valdymo plane numatytų priemonių neįgyvendinta (1.3 poskyris);

2.3. ministerija nustatė FVAIS ir FVIS kategorijas nesivadovaudama teisės aktuose numatytais kriterijais, todėl užtikrindama šių IS saugą taiko nepakankamas priemones (1.2 poskyris);

2.4. ministerijos kontrolės procedūros, užtikrinančios tinkamą pasirengimą nuosekliai ir efektyviai atkurti IS veiklą esant nenumatytoms situacijoms, nebuvo realiai išbandytos, todėl avarijos atveju ministerijoje nebūtų garantuota nuosekliai ir efektyviai atkuriama IS veikla, nenutrūkstamai teikiamos IT paslaugos (1.4 poskyris);

2.5. ministerijoje nėra elektroninės informacijos klasifikavimo aprašymo ir informacijos priskyrimo kriterijų, todėl suteikus prieigą prie elektroninių duomenų darbuotojams, kuriems šie duomenys nereikalingi atliekant tiesiogines pareigas, gali būti atskleista, sunaikinta arba pakeista Finansų ministerijos kaupiama informacija (1.2 poskyris).

3. Finansų ministerija neužtikrino efektyvaus VSAKIS kūrimo, nes sistema kurta nenustačius sistemos techninių reikalavimų ir ekonominio pagrindimo, kaip reikalauja teisės aktai, projekto įgyvendinimas vėlavo. Ne visi suplanuoti VSAKIS projekto tikslai pasiekti pilnai, o dalis ministerijos nustatytų projekto tikslų pasiekimo kriterijų buvo nedetalūs ir nepamatuojami (2.skyrius).

Rekomendacijos

Lietuvos Respublikos finansų ministerijai:

1. Siekiant, kad IT plėtra atitiktų ministerijos veiklos poreikius:

1.1. numatyti kontrolės priemones, užtikrinančias IT planavimo periodiškumą, patvirtinti ministerijos IT plėtros planą (1 išvada);

1.2. atnaujinti IT valdymo komiteto veiklą, įtraukiant į jį svarbiausių veiklos procesų savininkus ir vadovybės atstovą, ir užtikrinti komiteto veiklos periodiškumą (1 išvada).

2. Siekiant užtikrinti ministerijos valdomos informacijos saugą ir išvengti galimų veiklos sutrikimų:

2.1. atlikti IS saugos atitikties vertinimą (2.2. išvada);

2.2. nustatyti IS pokyčių valdymo tvarką (2 išvada);

2.3. patikrinti ministerijos veiklos tęstinumo valdymo plano veiksmingumą (2.4. išvada);

2.4. vadovaujantis teisės aktais nustatyti tinkamą FVIS ir FVAIS sistemų kategoriją ir atlikti jų rizikos vertinimą (2.3. išvada);

2.5. Saugos elektroninio tvarkymo taisyklėse nurodyti elektroninės informacijos, priskirtos tam tikrai kategorijai, sąrašus ir asmenis, atsakingus už šios informacijos tvarkymą (2.5. išvada);

2.6. parengti asmens duomenų tvarkymo taisykles ir inicijuoti ministerijos informacijos, esančios asmens duomenų valdymo registre, atnaujinimą (2.1. išvada).

3. Siekiant užtikrinti vykdomų IT projektų valdymo kokybę, patvirtinti bendruosius ministerijos IT projektų valdymo principus (3 išvada).